How To | Create A VPN Between An Allied Telesis Router And A Microsoft Windows XP[1] Client, Without Using NAT-T

1. Internet Explorer and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.

Introduction

This document describes how to provide secure remote access through IP security (IPSec) Virtual Private Networks (VPN).

This VPN solution provides your office with secure internet access and firewall protection, plus remote encrypted VPN access for staff who work from home.

You should use the companion Note *How To Create A VPN Between An Allied Telesis Router And A Microsoft Windows XP Client, Using NAT-T* instead, if:

- the Allied Telesis router is connected to the Internet through a NAT gateway device, such as an ADSL modem, and/or
- you want to let travelling staff connect to your office from such places as hotel rooms.

This companion How To Note is available from www.alliedtelesis.com/resources/literature/howto.aspx.

Consider the following typical scenario:

You are the manager of a small business and you have purchased an AR415S for your small office premises. You have five PCs networked together with a server in your office. You intend to use your AR415S as your Internet gateway and for it to provide firewall protection.

You also have people who sometimes work from home. You would like these staff members to have secure (encrypted) remote access through the Internet to the servers in your office, to allow them to access files, the private Intranet, and business email.

Each staff member has a laptop or PC with Windows XP installed.

This document describes how to configure the Windows system to use IPSec VPN to connect to your office through the AR415S router.

When your staff want to connect to the office they simply use the VPN icon on their desktop to initiate the IPSec VPN connection.

Which products and releases does it apply to?

The following Allied Telesis routers are most suitable as VPN gateways because they have fast hardware encryption support and high performance:

- AR415S, AR44xS series, and AR450S
- AR750S and AR770S

The AR415S achieves up to 90 Mbps throughput with 3DES or AES encryption.

You can also use older routers as VPN gateways, but they will not have as high performance. The older routers depend on either the Encryption Mini Accelerator Card (EMAC) or the Encryption PCI Accelerator Card (EPAC) to perform encryption. They include:

- AR725, AR745, AR720 and AR740 routers
- AR410 series routers
- AR300 series routers

Finally, you can also use the Rapier 24 and Rapier 24*i* switches as VPN gateways, but this is usually not a recommended practice. Doing so means you will lose wire-speed switching of data, because all traffic needs to be inspected by the firewall and IPSec at CPU processing speed.

Encryption algorithms such as 3DES and AES require a feature licence. This is included on some models. See your Allied Telesis representative for more information.

The configuration is supported on all AlliedWare versions since 2.3.1 and was tested using Microsoft Windows XP Professional or Home Edition, Service Pack 1a.

Related How To Notes

The following How To Notes give other VPN configurations for interoperating with a Microsoft Windows VPN client:

- *How To Create A VPN Between An Allied Telesis Router And A Microsoft Windows XP Client, Using NAT-T*
- *How To Create A VPN Between An Allied Telesis Router And A Microsoft Windows 2000 Client, Without Using NAT-T*
- *How To Create A VPN Between An Allied Telesis Router And A Microsoft Windows 2000 Client, Using NAT-T*

The following How To Notes give other VPN configuration examples:

- *How To Configure VPNs In A Corporate Network, With Optional Prioritisation Of VoIP*
- *How To Troubleshoot a Virtual Private Network (VPN)*
- *How To Configure A VPN Between Microsoft ISA Server 2004 And An Allied Telesis Router Client*
- *How To Use The Allied Telesis GUI Wizard To Create A Site-to-Site VPN Through A NAT Gateway Device*

- *How To Use The Allied Telesis GUI Wizard To Create A Site-to-Site VPN*
  (Use this Note when the VPN does not go through a NAT gateway device)
- *How To Create A VPN Between An Allied Telesis And A SonicWALL Router, With NAT-T*
- *How To Create A VPN Between An Allied Telesis And A NetScreen Router*
- *How To Configure Some Basic Firewall And VPN Scenarios*
- *How To Configure Some Advanced Features On Your ADSL Router*
- *How To Configure VoIP And Data Over A Meshed IPsec VPN*
- *How To Configure IPv6 Support For IPsec VPNs*

How To Notes are available from www.alliedtelesis.com/resources/literature/howto.aspx.

Security issue

Since this Windows VPN solution is usually used to allow remote access into corporate networks, a common security concern is "what happens if the remote laptop or PC is stolen or falls into unauthorised hands?" This is particularly a concern because the VPN connection is enabled through the standard dial-up networking window that allows username and passwords to be saved.

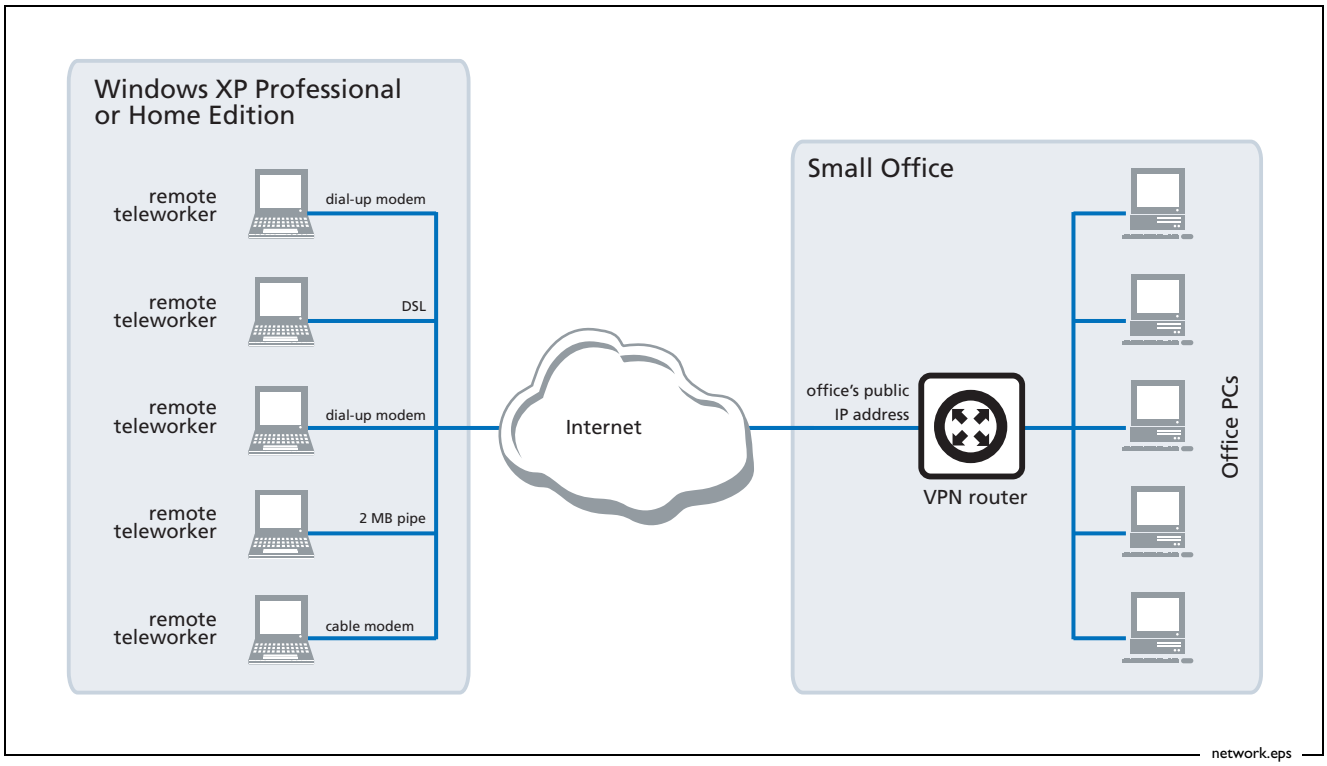
A solution to this security concern is to disable the standard behaviour that allows passwords to be saved. VPN users will then have to enter their password each time they connect.

If you would like to implement this security measure, refer to Microsoft Knowledge Base article 172430 by following this link: support.microsoft.com/default.aspx?scid=172430.

This solution works on both Windows 2000 and Windows XP.

Example network

The following figure shows an example of a network that could use this configuration.



Configuring the router

This section contains a script file for running IPSec encapsulating L2TP on a Head Office AR400 series router, configured to support IPSec remote PC clients.

Using this script involves the following steps:

1. "Perform initial security configuration on the router", on this page.
2. Make a copy the script, which starts on page 6. Name it (for example) *vpn.cfg*.
3. Personalise IP addresses, passwords etc in the script, so that they apply to your network. Placeholders for these are indicated in the script by text within < >.
4. Load the script onto the router using ZMODEM or TFTP.
5. "Set the router to use the configuration" on page 8.
6. Restart the router or activate the script.

Perform initial security configuration on the router

Before loading the configuration, you need to do the following steps.

1. Define a security officer.

   ```
   add user=secoff password=<your-password> priv=securityofficer
   ```

   This command must be in the configuration script as well.

2. Enable system security. Unless you do this, rebooting the router destroys encryption keys.

   ```
   enable system security
   ```

3. Log in as the security officer.

   ```
   login secoff
   ```

4. Generate a random key.

   ```
   create enco key=1 type=general value=<alphanumeric-string>
   ```

   Note the value of the string you have entered so that you can load it on the PC clients. This shared key will be used to encrypt ISAKMP negotiation.

The configuration script

Note: Comments are indicated in the script below using the # symbol.
Placeholders for IP addresses, passwords, etc are indicated by text within < >

```
set system name="IPSec Gateway"

# The command below shows the Security Officer inactive timeout delay.
# The default is 60 seconds. During setup you can instead use 600
# seconds if desired.

set user securedelay=600

# The incoming L2TP calls will be CHAP authenticated.
# They may be authenticated against the router's user database as
# configured below, or against a RADIUS Server if configured.
add user=dialin1 pass=friend1 login=no
add user=dialin2 pass=friend2 login=no
add user=dialin3 pass=friend3 login=no
add user=dialin4 pass=friend4 login=no
add user=secoff pass=<your-password> priv=securityOfficer login=yes
set user=secoff description="Security Officer Account"

# If RADIUS server support is needed, use a line such as this:
# add radius server=<your-RADIUS-server-address> secret=<secret-key>

# All dynamic incoming L2TP calls will associate with this PPP template
# as indicated below.

create ppp template=1 bap=off ippool="ip" authentication=chap echo=10
   lqr=off

# To cater for dynamic creation of incoming L2TP calls enter the
# following commands.
enable l2tp
enable l2tp server=both
add l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1

# The IP address allows for any valid Internet address.
enable ip
add ip int=vlan1 ip=<office-private-LAN-address>
add ip int=eth0 ip=<office-Internet-address> mask=<appropriate-mask>

# The default route to the Internet.

add ip route=0.0.0.0 mask=0.0.0.0 int=eth0
   next=<your-Internet-gateway-or-ISP-next-hop-address>

# The IP pool addresses are the internal address ranges you want to
# allocate to your IPSec remote PC clients
# (e.g. ip=192.168.8.1-192.168.8.254).

create ip pool=ip ip=<pool-range>
```

```
# Firewall
enable fire
create fire poli=main
create fire poli=main dy=dynamic
add fire poli=main dy=dynamic user=ANY
add fire poli=main int=vlan1 type=private

# Dynamic private interfaces are accepted from L2TP, which are from
# IPSec only.
add fire poli=main int=dyn-dynamic type=private
add fire poli=main int=eth0 type=public

# The firewall allows for internally generated access to the Internet
# through the following NAT definition.
add fire poli=main nat=enhanced int=vlan1 gblint=eth0

# This NAT definition allows Internet access for remote VPN users by
# providing address translation.
add fire poli=main nat=enhanced int=dyn-dynamic gblint=eth0
add fire poli=main rule=1 int=eth0 action=allow prot=udp
   ip=<office-Internet-address> port=500
   gblip=<office-Internet-address> gblpo=500

# Rule 2 becomes the L2TP tunnel allow rule. Additional security is
# provided by only allowing traffic from IPSec tunnels.
add fire poli=main rule=2 int=eth0 action=allow prot=udp
   ip=<office-Internet-address> port=1701
   gblip=<office-Internet-address> gblpo=1701 encap=ipsec
create ipsec sas=1 key=isakmp prot=esp encalg=3desouter hashalg=sha
   mode=transport
create ipsec sas=2 key=isakmp prot=esp encalg=3desouter hashalg=md5
   mode=transport
create ipsec sas=3 key=isakmp prot=esp encalg=des hashalg=sha
   mode=transport
create ipsec sas=4 key=isakmp prot=esp encalg=des hashalg=md5
   mode=transport

# The ORDER of proposals is important. You should propose the strongest
# encryption first.
create ipsec bundle=1 key=isakmp string="1 or 2 or 3 or 4"
create ipsec policy=isakmp int=eth0 action=permit lport=500 rport=500

# This is a generic IPSec policy that multiple IPSec remote PC clients
# can connect through.
create ipsec policy=to_HQ int=eth0 action=ipsec key=isakmp bundle=1
   peer=any isa=keys
set ipsec policy=to_HQ transport=udp rport=1701

# The following policy allows for internally generated Internet access.
create ipsec policy=Internet int=eth0 act=permit
enable ipsec
create isakmp policy=keys peer=any key=1
set isakmp policy=keys sendd=true
enable isakmp
```

Set the router to use the configuration

After loading the configuration onto the switch, set the router to use the script after a reboot. If you named the script vpn.cfg, enter the command:

```
set conf=vpn.cfg
```

If you entered the configuration directly into the command line instead of loading the script, save the configuration by entering the commands:

```
create conf=vpn.cfg
```

```
set conf=vpn.cfg
```

Configuring the VPN client

Configuring the Windows XP VPN client involves the following two stages:

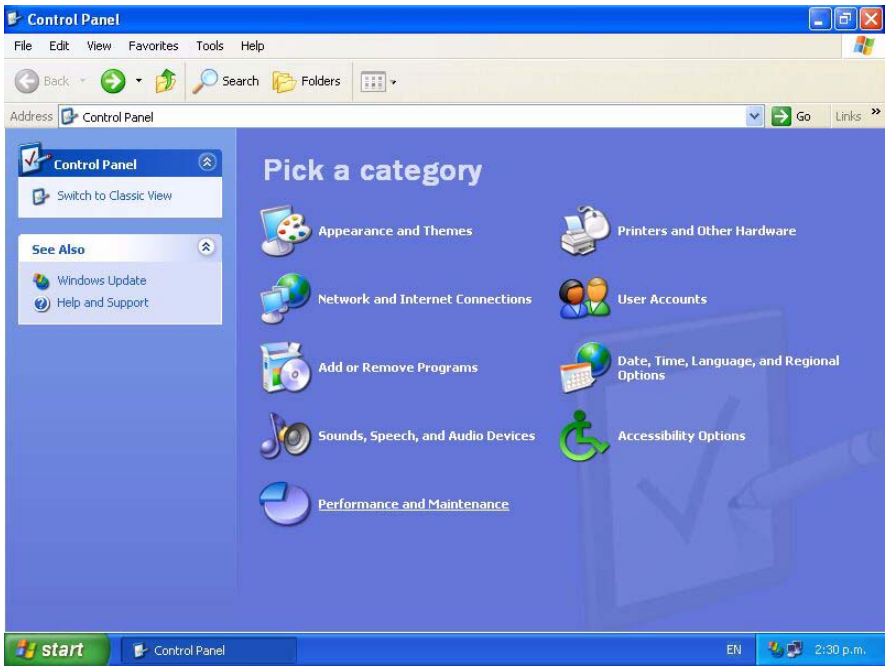
- "Create a VPN tunnel from the PC host to the router", on this page
- "Connect to the Head Office" on page 12

Create a VPN tunnel from the PC host to the router

Note: You need to know the public IP address for the router from your Internet Service Provider (ISP) for this configuration.
This example assumes that you have already set up your internet connection.

1. On your desktop, click *Start* > *Control Panel*.

   Make sure you are in *Category View*, as shown in the following figure. If your computer is in Classic View, click **Switch to Category View** in the Control Panel Menu on the left of your screen.



2. Click *Network and Internet Connections* > *Create a connection to the network at your workplace*.

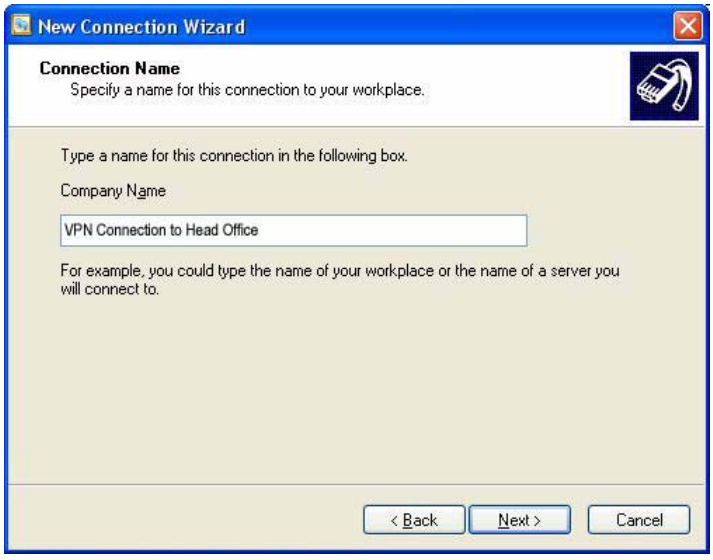
   This starts up the New Connection Wizard.

   Select *Virtual Private Network Connection* as shown in the following figure.

New Connection Wizard
Network Connection
How do you want to connect to the network at your workplace?
Create the following connection:
Dial-up connection
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
Virtual Private Network connection
Connect to the network using a virtual private network (VPN) connection over the Internet.
< Back
Next >
Cancel

3. Click **Next**.

   Type in a name for the connection (e.g. VPN Connection To Head Office) as shown in the following figure.


New Connection Wizard
Connection Name
Specify a name for this connection to your workplace.
Type a name for this connection in the following box.
Company Name
VPN Connection to Head Office
For example, you could type the name of your workplace or the name of a server you will connect to.
< Back
Next >
Cancel

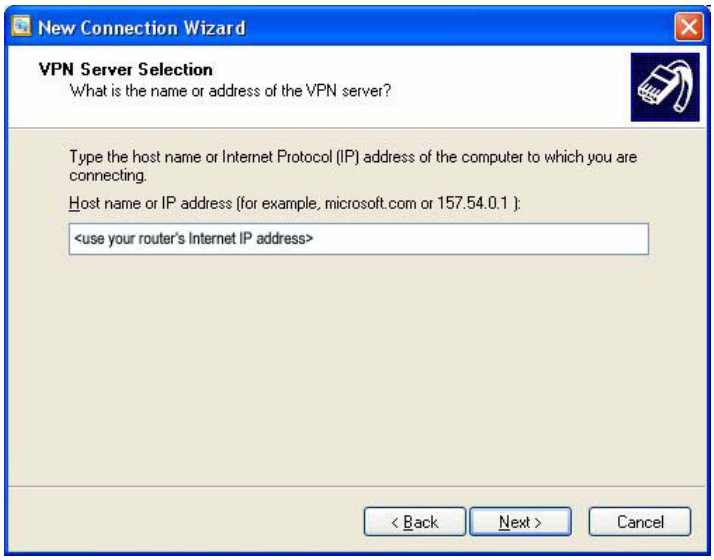
4. Click **Next**.

   Assign an associated dialled call or select *Do not dial the initial connection*. Selecting *Do not dial the initial connection* is appropriate if you will have LAN access available before initiating the VPN call (for example, if you have a cable modem).

New Connection Wizard
Public Network
Windows can make sure the public network is connected first.
Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.
Do not dial the initial connection.
Automatically dial this initial connection:
< Back
Next >
Cancel

5. Click **Next**.

   Enter the name or IP address of the office router. This will be its Public Internet address, which the ISP will have allocated you.


New Connection Wizard
VPN Server Selection
What is the name or address of the VPN server?
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.
Host name or IP address (for example, microsoft.com or 157.54.0.1):
<use your router's Internet IP address>
< Back
Next >
Cancel

6. Click **Next**.

   You have now completed creating the connection, as shown in the following figure. If you want to, check the *Add a shortcut to this connection to my desktop* check box. Then click **Finish**.

New Connection Wizard
Completing the New Connection Wizard
You have successfully completed the steps needed to create the following connection:
To Head Office
• Share with all users of this computer
The connection will be saved in the Network Connections folder.
Add a shortcut to this connection to my desktop
To create the connection and close this wizard, click Finish.
< Back
Finish
Cancel

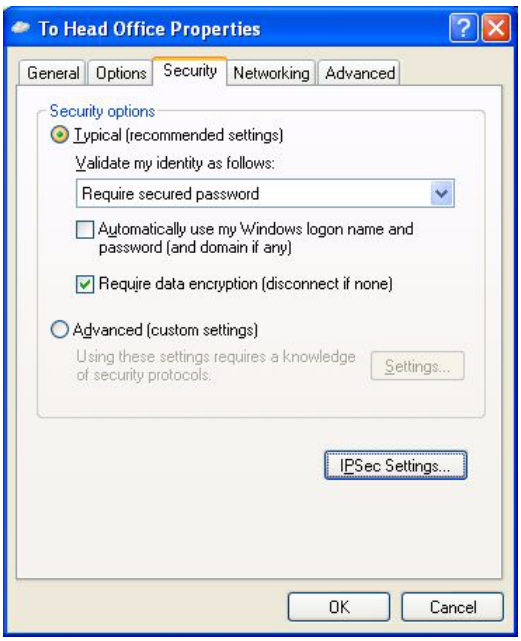
Connect to the Head Office

1. Double-click the new *Head Office* icon on your desktop or in "Network Connections" in the control panel.

2. Enter your **user name** and **password** as shown in the following figure. These are the user name and password that is (or will be) configured on the router's user database or RADIUS server.

3. Click **Properties**.

   This opens the *Head Office Properties* window. Click the **Security Tab,** as shown in the following figure.



4. Click the **IPSec Settings** button.

   This opens the *IPSec Settings* window, as shown in the following figure. Select the *Use pre-shared key for authentication* checkbox and enter your **pre-shared key**. The pre-shared key needs to be the same ISAKMP pre-shared key as is defined on the router ("Generate a random key." on page 5).

5. Click **OK**.

   This returns you to the *Head Office Properties* window.

6. Click the **Networking Tab**, as shown in the following figure. In the *Type of VPN* drop-down box, select *L2TP IPSec VPN*.

7. Click **OK.** This completes the configuration of the L2TP client. To connect to the office, click **Connect**. Note that the connection will fail if the router has not yet been configured.

Testing the tunnel

The simplest way to tell if traffic is passing through the tunnel is to perform a traceroute from the Windows XP client to a PC in the router's LAN. To do this, use the following command at the command prompt on the Windows XP client:

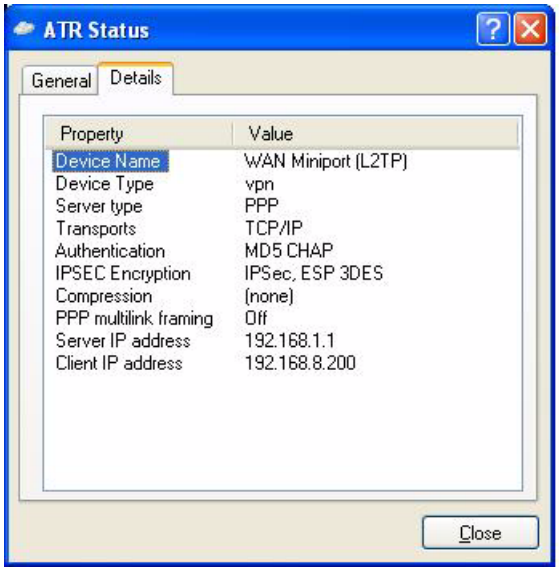
```
tracert <ip-address>
```

If traffic goes through the tunnel, the traceroute may display IP addresses from one or both peers' private networks and public interfaces. If it shows other public IP addresses, then traffic is not passing through the tunnel.

Checking the connection from the Windows client

To check your connection details, right-click on your connection icon (e.g. Virtual Private Connection to Head Office) in the Network Connections folder, or on your desktop.

Click **Status**. Then click the **Details** tab to check your connection information, as shown in the following figure.



Troubleshooting

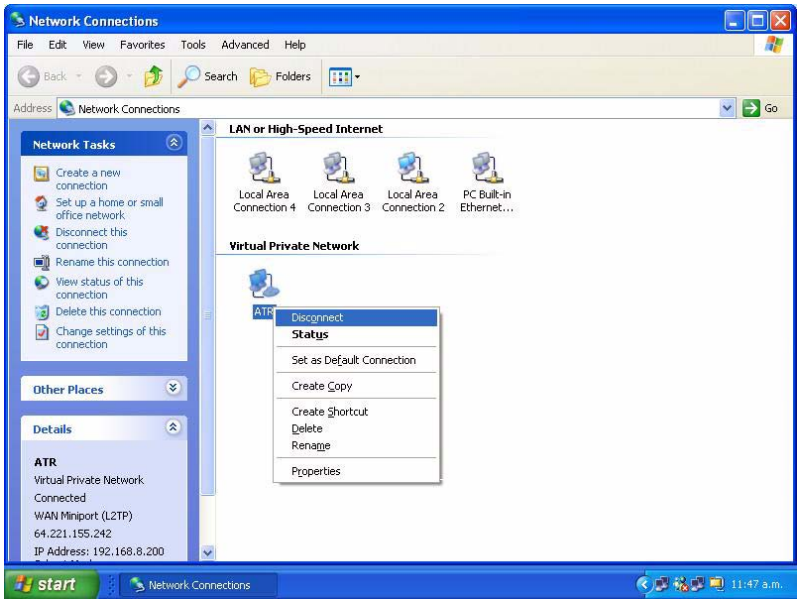
If your tunnel is not working, see the How To Note *How To Troubleshoot A Virtual Private Network (VPN)*.

This How To Note has detailed information about testing and troubleshooting VPNs on the router.

Closing the connection

To close your connection, right-click on your connection icon and click **Disconnect**. The following figure shows this.

.



USA Headquarters | 19800 North Creek Parkway | Suite 200 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
European Headquarters | Via Motta 24 | 6830 Chiasso | Switzerland | T: +41 91 69769.00 | F: +41 91 69769.11
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
www.alliedtelesis.com

© 2007 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. Allied Telesis is a trademark or registered trademark of Allied Telesis, Inc. in the United States and other countries. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.

C613-16003-00 REV C

Connecting The IP World

Allied Telesis